Montgomery County Government
Information Technology Architecture

Department of Technology Services
Montgomery County Government, MD

Public Version

VERSION	DATE	DESCRIPTION	AUTHOR
1.0	10 October, 2003	Document Created	Deepak Bhatnagar, Montgomery County Government
2.0	24 September, 2004	Version Released	Gretchen Hurley, ASSYST, Inc.
3.0	16 December, 2005	Version Released	Dianne Lafleur, ASSYST, Inc.
4.0	29 March, 2007	Minor corrections	Mike Tarquinio, Montgomery County Government
4.0	26 April, 2007	Update deployment domain	Mike Tarquinio, Montgomery County Government
4.0	30 April, 2007	Update AD&SSO and Mainframe	Mike Tarquinio, Montgomery County Government
4.0	10 May, 2007	Update AD&SSO	Mike Tarquinio, Montgomery County Government
4.0	10 May, 2007	Update Email System Services	Mike Tarquinio, Montgomery County Government
4.0	14 May, 2007	Update EHI Section	Mike Tarquinio, Montgomery County Government
4.0	30 May, 2007	Update DCM Section	Mike Tarquinio, Montgomery County Government
4.0	26 July, 2007	Update System Operations Domain	Mike Tarquinio, Montgomery County Government
4.0	3 August, 2007	Update GIS Domain	Mike Tarquinio, Montgomery County Government
4.0	5 September, 2007	Update Network Domain and review comments	Mike Tarquinio, Montgomery County Government
5.0	17 December, 2007	Add Team Collaboration Service & remove machine names	Mike Tarquinio, Montgomery County Government
6.0	4 February, 2008	Add CM Tools Service and Enterprise Server Management	Mike Tarquinio, Montgomery County Government
7.0	20 August, 2008	Added SaaS and Portal services. Updated Security, Network, PBX, and Record Management domains. Added service owners.	Mike Tarquinio, Montgomery County Government
8.0	27 October, 2008	Changes to reflect Security Team	Mike Tarquinio, Montgomery County Government

		concerns	
9.0	25 November, 2008	Review Comments	Mike Tarquinio, Montgomery County Government
10.0	3 March, 2009	Review Comments	Mike Tarquinio, Montgomery County Government

Table of Contents

1.0 Introduction

Montgomery County takes advantage of mature technologies in areas of data, voice and radio networking, datacenter operations and monitoring, hardware and software systems deployment, and application development. This document, prepared by the Department of Technology Services (DTS), is used as a comprehensive reference to the County's information technology architecture.

The Information Technology Architecture Document is DTS' framework for program execution. It is prepared in concert with the DTS Strategic Plan and is designed to support the initiatives outlined in the plan.

The County has three essential organizational resources, people, process and technology. People are the County's greatest resource, Process binds them together into a coherent workforce, and Technology is the tool. This document addresses the technology component.

1.1 Purpose

The purpose of this document is to present well-defined, strategic standards adopted for the development and delivery of the County's information systems. It provides a cohesive blueprint to optimally design, purchase, develop, deploy and manage information systems for the County. The components of the overall infrastructure are shown in Figure 1-1 – Information Technology Framework.

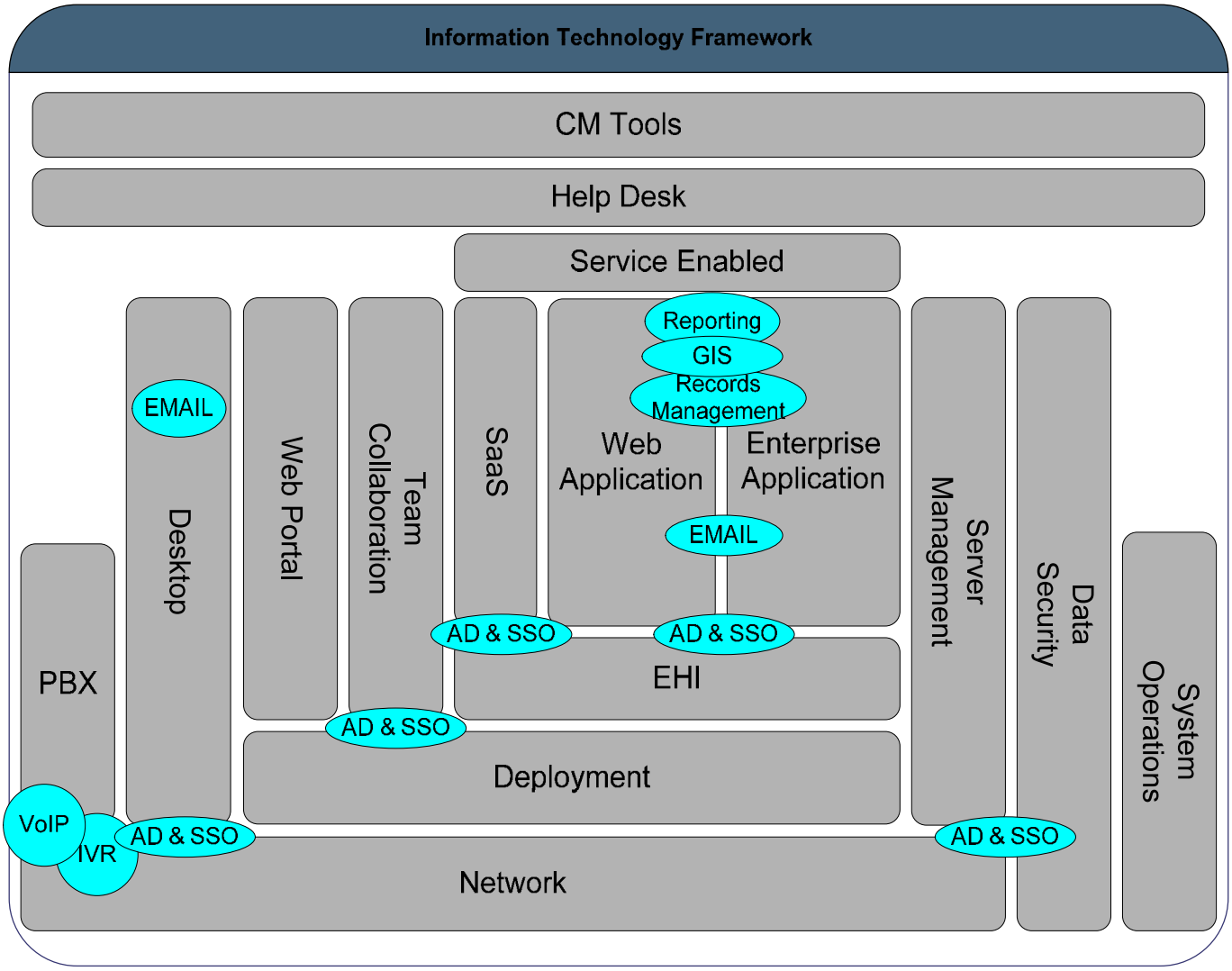


Figure 1-1 Information Technology Framework

This integrated approach to developing complimentary technologies yields a rapid return on investments for new and upcoming programs. In certain areas, the County benefits from consolidating technology, increasing depth of knowledge and skill-set, and lowering the total cost of ownership.

The architecture is designed to achieve efficiencies based on economies of scale. Standardization of technologies encourages the development and purchase of reusable infrastructure and business components. This enhances in-house employee skills in a predictable set of hardware, systems software, COTS packages, and communication and networking platforms. Tiered architecture permits horizontal scaling of solutions by rapid allocation of skills and resources.

This document identifies a framework for the County's IT initiatives with a great degree of specificity. It also offers a certain amount of flexibility, permitting Program Managers a list of options for the development of their enterprise software solutions.

1.2 Document Format

As Figure1 suggests, Montgomery County Technical Architecture may be defined as a collection of the following components architectures:

- Active Directory and Single Sign On Services - enabling security
- Data Security Domain - implementing secure access control management
- Desktop Domain - defining desktop computing standards
- Email Domain - increasing operational efficiencies
- Help Desk - providing assistance to the County
- Geographic Information System– delivering cartographic data and location services
- Record and Document Management Domain - advancing automation
- Reporting Domain– optimizing software licenses
- Enterprise Applications Domain - automating business processes
- Web Applications Domain – developing and deploying applications rapidly
- Service Enabled Domain – avoiding stovepipe applications
- Deployment Domain - utilizing resources and sharing costs
- Mainframe Application Services - integrating core business processes
- Network Domain - empowering common infrastructure
- Cabling Requirements and Standards Domain
- PBX Domain - supplying quality landline services
- Interactive Voice Response Domain - integrating IT and Telephony
- Enterprise Hosting Infrastructure Domain - hosting enterprise applications
- System Operations Domain – Data Center Operations including Backup Services
- Team Collaboration Domain – providing group collaboration
- Configuration Management (CM) Tools Domain – providing CM Tools Support
- Enterprise Server Management Domain – providing Enterprise Server Management
- Software as a Service (SaaS) – providing support for SaaS applications
- Web Portal Domain – providing Internet and Intranet web portals

Each architectural component identified above introduces the following topics:

Principles – explaining the purpose of the component, along with some implementation details.

Owners – identifies both the technical and business owners for the component.

Components – expanding on the operational aspects of the component by identifying preferred implementation products and staff skill-sets.

Standards and Guidelines – identifying standards and guidelines which the County follows so that it can provide quality services.

The County has assembled information detailing its technologies and its direction. Two versions of the document will be published. One version will have reduced information and will be for public access. The complete version will be available to only selected Montgomery County Employee populations as

well as for Vendors involved in certain Technology Request for Proposals. To avoid releasing potentially sensitive information the county follows a strict release process that involves review at multiple levels (See Section 10-617(g) of the Maryland Public Information Act).

The owner of this document is Mike Tarquinio (michael.tarquinio@montgomerycountymd.gov) the Department of Technology Service Enterprise Architect. The Department is located at the Department of Technology Services, 101 Monroe Street, 13th Floor, Rockville, Maryland 20850.

1.3 Montgomery County Technology Governance

The Department of Technology Services provides Information Technology Services to Montgomery County. The County Code, Chapter 2, Division 11D outlines the functions and duties of the Department of Technology Services.

1.3.1 Department of Technology Services Purpose

As defined in the county code the purpose of the Department of Technology Services is to:

(1) promote the appropriate use of automated information systems and telecommunications technology by the County government;

(2) plan, develop, and ensure the proper operation of the County government's telecommunications capabilities, with special emphasis on the long-term issues of connectivity and compatibility;

(3) ensure that the County government provides automated information services;

(4) review decentralized process support systems for consistency with overall policy and compatibility with other governmental systems; and

(5) promote the sharing of data and information technology systems among the departments and agencies, subject to the state public records act.

1.3.2 Department of Technology Services Duties

As defined in the county code the duties of the Department of Technology Services are to:

(1) operate the County's central computer system and provide technical support necessary to:

(A) generate and maintain the software of all systems;

(B) assess requirements for computer hardware and software; and

(C) supervise network control activities;

(2) administer each cable communications or other telecommunications franchise granted by the County Council and any other telecommunications agreement involving or regulated by the County;

(3) operate and manage all telecommunications facilities owned or controlled by the County, including the County fiber-optic data network, telephone system, Internet service, cable television transmissions, and public safety communications;

(4) make County policy recommendations;

(5) establish standards for automated information systems and telecommunications;

(6) plan and oversee the installation and support of departmental and enterprise automated information systems, including public safety communications systems, local- and wide-area networks, enterprise servers, and the desktop computer replacement program, under written policies approved by the Chief Administrative Officer (CAO);

(7) maintain a geographic database of all installed telecommunications facilities in the County for which the County has any legal authority to require data, or is able to obtain voluntarily or through a third-party;

(8) approve, deny, or modify all requests for telecommunications and information processing facilities before acquisition; and

(9) advise the County Council on the acquisition of telecommunications and information processing systems, although the Council has the final authority to acquire facilities and systems for its own use.

1.3.3 Chief Information Officer Responsibilities

As defined in the county code the Director of Technology Services serves as the County's Chief Information Officer (CIO). The CIO, under the supervision of the Chief Administrative Officer, must:

(1) serve as chair of the Information Technology Policy Advisory Committee (ITPCC);

(2) review and approve any proposed procurement of information technology for the County government to ensure that the proposed procurement is consistent with approved information technology policies and standards, unless the Director of Procurement appeals the CIO's decision to the Chief Administrative Officer to resolve;

(3) plan, direct, and manage each major information technology project of the County government, under written policies approved by the CAO;

(4) submit a plan to the County Council by February of each year for the County's use of any information technology resources that a person was required to provide under a cable or other telecommunications franchise granted by the Council under Chapters 8A or 49;

(5) administer each cable television or other telecommunications franchise granted by the Council strictly according to law, the approved franchise agreement, and any franchise administration policies established by the Council by resolution;

(6) provide technical assistance to the ITPCC or any successor organization;

(7) serve as the County government's liaison with other County, State, regional, and federal government agencies, such as the Montgomery County Public Schools, Montgomery College, the Washington Suburban Sanitary Commission, and the Maryland-National Capital Park and Planning Commission, to promote efficiency and, to the extent practical, consistent standards and interoperability of information technology among the County government and these agencies; and

(8) perform the duties described in Section 2-58E to coordinate all telecommunications transmission facilities in the County.

1.3.4 Information Technology Policy Advisory Committee

(1) The Information Technology Policy Advisory Committee (IPAC) includes:

(A) the Director of Finance;

(B) the Director of the Office of Management and Budget;

(C) the Director of the Office of Procurement;

(D) the Director of the Office of Human Resources;

(E) the County Attorney;

(F) The Chief of Police;

(G) the Director of Fire/Rescue Services;

(H) the Director of Public Works and Transportation;

(I) the Director of Health and Human Services; and

(J) any other head of a County agency, department, or office listed in Executive regulations approved under method 2.

(2) The members listed in paragraph (1) serve as permanent, *ex officio* voting members.

(3) The Committee must:

(A) establish and frequently review, at least twice a year, information technology policies and standards for the County government that:

(i) promote efficient delivery of government services to the public;

(ii) are cost-effective;

(iii) promote, to the extent practical, interoperability with other public and private information technology systems;

(iv) ensure the accuracy, integrity, and security of information created by or entrusted to the County government; and

(v) comply with federal, State, and local laws;

(B) monitor information technology developments and promptly advise the Executive and Council about potential impacts of new technology;

(C) review and advise the CIO on any proposed procurement of information technology for the County government that exceeds an amount established by Executive regulation; and

(D) make recommendations to the CIO regarding the use of any information technology resources that a franchisee was required to provide under a cable television or other telecommunications franchise granted by the Council. (1987 L.M.C., ch. 34, § 2; 2002, L.M.C., ch. 5, § 1.)

1.3.5 Technical Operational Management Group (TOMG)

The Technical Operational Management Group (TOMG) is a group of County information technology managers appointed by their respective department heads to provide technical and operational review of information technology issues that are brought before the IPAC. Regularly scheduled meetings provide a forum for the exchange of information and ideas.

1.3.6 Technical Architecture Document Change Management

The Montgomery County Government Information Technology Architecture document is published by the DTS Enterprise Architect. The Enterprise Architect is responsible for working with DTS Content Experts and department representatives (through TOMG) to create a coherent Technical Architecture. The document adheres to stringent change management controls and follows a defined change management process.

Change requests can be initiated via DTS content experts, TOMG members, or the DTS Enterprise Architect. Contact the DTS Enterprise Architect Mike Tarquinio (michael.tarquinio@montgomerycountymd.gov) for further details.

1.4 References

1. Montgomery County Office of Management and Budget – Administrative Procedure 6-1, June 14, 2004; *Use of the County-Provided Internet, Intranet, and Electronic Mail Services*;

2. Montgomery County Office of Management and Budget – Administrative Procedure 6-6, May 4, 2005; *Information Technology Policies and Procedures*;

3. Montgomery County Office of Management and Budget – Administrative Procedure 6-7, May 4, 2005; *Information Resources Security*;

4. Montgomery County Department of Technology Services, September 2004; *Computer Security Guideline*;

5. Montgomery County Department of Technology Services, September 2004; *DTS Strategic Update 2006 - 2007*;

6. Montgomery County Government, May 31, 2007; *Montgomery County Code*;

7. Montgomery County Department of Technology Services, July 19, 2007; *Enterprise Architecture Configuration Management Plan*

8. Montgomery County Department of Technology Services, April 14, 2008; *Montgomery County Government Public Safety Information Technology Architecture*

2.0 Active Directory (AD) and Single Sign On (SSO) Services

2.1 Principles

Microsoft's Active Directory (AD) is used to authenticate users, and to allow them into the County network. Single Sign On (SSO) services is an enterprise strategy designed to minimize administration and user authentication stress, eliminate multiple userids and multiple passwords. The Single Sign On service is implemented through Tivoli Access Manager (TAM) and Active Directory. With AD and TAM, users are able to log on to the network, and log into specific SSO configured applications as the need arises. For example, once the user is logged into the network, the user is not required to log into Exchange to access the County's email system.

2.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

3.0 Cabling Requirements & Standards

3.1 Principles

The County's goal is to standardize its cabling infrastructure to promote faster speed, better communication, easier troubleshooting, and less need for repair. DTS Telecommunications offers connectivity for telecommunications equipment throughout the County. Cable installation services are offered by the County and by outside Contractors.

3.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Service Team.

4.0 Data Security Domain

4.1 Principles

Security is an essential part of every component in the County's IT Architecture framework with multiple domains and groups having responsibilities. The Security Domain includes not only technology but process and procedures and is present through all aspects of system acquisition and development.

The following domains have Security responsibilities:

- Active Directory and Single Sign On – Centralized Directory Service supporting Single Sign On Services
- Deployment Domain – Common Enterprise Server configurations and patch management services
- Desktop Domain – Centralized desktop management with common configurations, patch management services, lockdown policy, centralized anti-virus and anti-spyware services
- Email System Services – Centralized mail service including anti-virus, anti-spyware and spam removal services
- Enterprise Hosting Infrastructure – Secure hosting infrastructure
- Help Desk Services – Centralized help desk that supports Incident Response
- Network Domain – Enterprise network that includes protected single point of access, internal and external firewalls, wireless security, and network segmentation services
- Service Enabled Domain – Use of an Enterprise Service Bus for centralized secure information transfers
- System Operations Domain – Centralized Data Center that includes redundant systems for high availability and physical security measures
- Configuration Management – Centralized Configuration Management systems for protection of project assets.
- Enterprise Server Management – 24x7 server monitoring
- Security Domain – Includes polices and procedures, risk management practices, Virtual Private Network access, and operational security monitoring including security scanning, policy enforcement, and log correlation.

4.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Security Team
- DTS Core Systems Team
- DTS Server Team
- DTS Client Computers (DCM) Team
- DTS Network Services Team

- DTS Data Center Operations Team
- DTS Enterprise Architect
- DTS Help Desk Services

5.0 Deployment Domain

5.1 Principles

The Deployment Domain consists of server hardware, operating systems, middleware and personnel. The goals of the Deployment Domain are to:

- Provide robust and stable IT environments.
- Maintain a continual pool of spare server capacity, which can be used for new deployments, horizontal scaling and sparing.
- Provision new server and middleware environments in near real time.
- Research and adopt new tools and building blocks to lower Total Cost of Ownership (TCO).

Progress of the last few years includes:

- Migration from RISC/ Mainframe computing to midrange Intel x86 servers.
- Implementation of Virtual Machine (VM) on Intel x86 servers.
- Increased deployment of “Open Source” operating systems and middleware.

Successful operational procedures include:

- In-house web mastering of technical documentation and dashboards.
- Routine auditing and upgrading of system patch levels, anti-virus engines and backups.
- Automation of routine operations and monitoring.
- Detailed peer reviews prior to new deployments.

5.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team

6.0 Desktop Domain

6.1 Principles

Desktop Computer Modernization is a centralized program for the planning, acquisition, asset management, and support services associated with desktop computers. Desktop Computer Modernization (DCM) is part of the Department of Technology Services (DTS). Under this program, the County uses its own in-house personnel for integrated desktop planning, and a single external service provider for desktop acquisition assistance, asset management, and support services. Through the implementation of DCM, the County achieves several key goals:

- Brings current technology to the desktop
- Reduces the cost of and need for support services through planning
- Provides a single source of support through a centralized single point of contact IT Help Desk
- Provides quality services to end users in an accurate, consistent, timely and professional manner
- Controls total cost of ownership.

6.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Client Computers (DCM) Team.

7.0 Email System Services

7.1 Principles

The County uses Microsoft Exchange for its enterprise email system. This system supports Enterprise wide email functions to employees within the County core office buildings, and locations anywhere around the world. Access is allowed via the Outlook desktop client, Outlook Web Access (OWA) web browser and Blackberry devices. Mailbox stores are managed centrally, and backed up at the server level (not at the brick level). Administration is both centralized and decentralized depending on the specific department and need. Anti-Spam processing and filtering for inbound mail is supplied by two Spam Protection Appliances.

7.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

8.0 Enterprise Application Domain

8.1 Principles

Enterprise Applications are developed to encapsulate the County's business processes. Enterprise processes focus on an enterprise's core business functions (human resources, finance, public safety and accounting). Enterprise Applications enabling core operational aspects of the County will be implemented as Web-enabled solutions. The end user will be presented with an intuitive graphical user interface (GUI) on their Web browser, often referred to as a 'thin client' since it does not require any client desktop deployment.

8.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Enterprise Architect
- DTS Enterprise Services Architect

9.0 Enterprise Hosting Infrastructure Platform

9.1 Principles

The Enterprise Hosting Infrastructure (EHI) is the framework the County uses to deploy its enterprise applications. The County's EHI goals are to integrate business processes across the County by integrating and extending existing web applications. The County benefits from EHI because it promotes enterprise-wide data standardization, reuse, interoperability, and information management across applications and agencies. Reducing cost and development time, EHI facilitates common solutions for business processes, lower operational costs, increased business productivity, and better utilization of resources.

EHI encompasses most components of the County's IT Framework: Enterprise Application Domain (see Chapter 8), Web Application Domain (see Chapter 21), Software as a Service (see Chapter 25), Deployment Domain (see Chapter 5), Network Domain (see Chapter 14), Security Domain (see Chapter

4), Reporting Domain (see Chapter 18), Geographic Information Systems Domain (see Chapter 10), Help Desk (see Chapter 11), Active Directory & Single Sign On (see Chapter 2), Email System Services (see Chapter 7), Service Enabled Domain (see Chapter 19), Enterprise Server Management (Chapter 24) and System Operations Domain (see Chapter 20). Figure 9-1 demonstrates the components that make up the County's EHI.

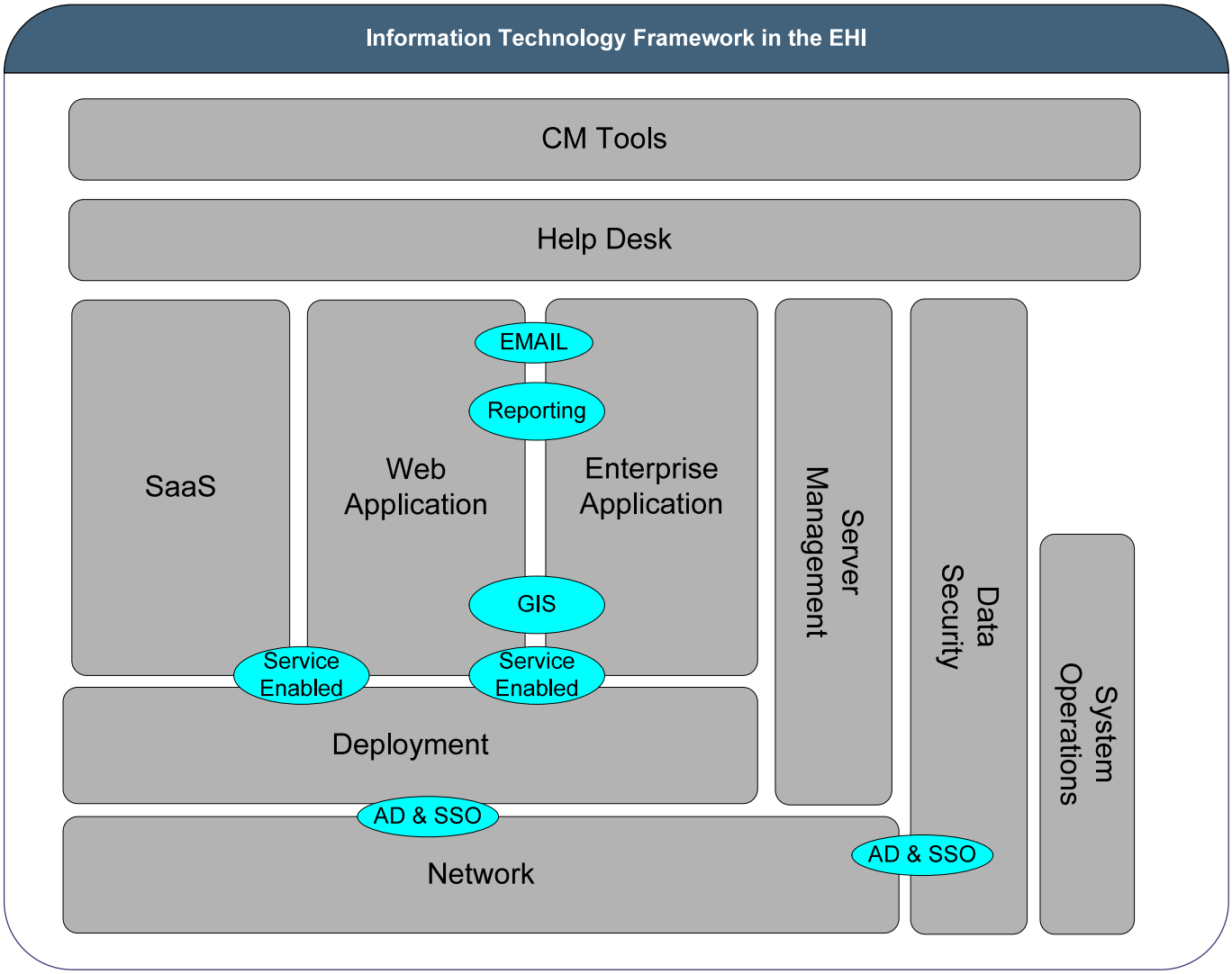


Figure 9-1 Enterprise Hosting Infrastructure Components

When a new application is targeted to be hosted in the EHI an intake form is filled out for the application. The intake form contains information about the application with one aspect of the information being the NIST Confidentiality, Integrity and Availability requirements for the application.

9.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Enterprise Architect
- DTS Enterprise Services Architect

10.0 Geographic Information Systems Domain

10.1 Principles

The County has designed and implemented a Geographic Information System (GIS) to deliver geospatial data to spatially enabled desktop, Web-based applications, and location services. The system generates hard copy and Web-based cartographic/mapping presentations enabling data analysis and decision support services. The County has dedicated resources to create, maintain, manage, and store geo-spatial data.

The County has two definitions of spatially enabled services. One is a service capable of integrating spatial data with other business data across multiple, heterogeneous data sources. The other is a service supporting abstract data types (images, text, and spatial data) spatial operators, functions, and spatial locator indexes. The County implements Environmental Systems Research Institute's (ESRI) GIS data models and software. The County has migrated about 75% of its GIS assets from the Workstation ArcInfo data model to Desktop ArcGIS, the new ESRI GIS software platform.

10.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS GIS Team.

11.0 Help Desk Services

11.1 Principles

The IT Help Desk provides a single point-of-contact, centralized support to County employees and contractors using the County's IT Infrastructure. The IT Help Desk resolves problems or, as needed, routes problems to other support organizations to assure that they are resolved properly.

11.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Help Desk Services Team.

12.0 Interactive Voice Response Domain

12.1 Principles

The Department of Technology Services' goal is to develop IVR and Customer Relationship Management (CRM) strategies that improve customer service and lower operational cost by integrating all County IVR and CRM functions into one enterprise platform. The current platform will expand to accommodate a variety of applications, reduce application redundancy, and service the County in a more efficient way.

Interactive Voice Response (IVR) is a technology that enables callers to obtain information stored in a corporate database. IVR technology uses the familiar telephone keypad as an information retrieval and data gathering conduit. Recorded voice messages prompt and respond to caller inquiries and commands.

IVR's functions range from the simple process of selecting options stored in a computer (such as the single digit menus deployed throughout the County), to more complex interactive exchanges that rely on database lookups, such as the Finance Department's tax line script, and Health and Human Services' payment status system.

12.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Services Team.

13.0 Mainframe Application Services

13.1 Principles

Montgomery County Government owns and operates an IBM mainframe to support the County's legacy applications, which are General Ledger, Payroll, Purchasing, Fixed Assets, Budget and Tax Assessment.

The mainframe is an IBM Z9 BC Type-Model 2096-R07 B03 three processor 109 MIPS machine with one Crypto Express2 and one DB2 zIIP sub processor. It is running the z/OS v1.9 Operating System. Additional hardware details are:

- DASD - IBM 2105-F20 SHARK
- Tape System – one 3420 reel-to-reel drive, 3480, 3490, and 3590 cartridge drives
- Printers – two Xerox DP75 printers and one IBM 6202 impact printer

- Communications – One 3745 communications front end processor and three 2216-400 routers

Connections for all the printers, SHARK DASD, 3480 and 3490 tape drives are all via ESCON connections. The 3590 tape drives use a FICON connection.

System software supported on the mainframe include:

- CA-ACF2 Rel 12 security
- CA-7 v11.5 job scheduler
- CA-1 v11.5 tape management system
- CA-Opera v3.1 automated systems manager
- CA-Librarian v4.3 source code management
- DB2 v8.1
- CICS TS 3.1
- IMS DB/DC 8
- SAS v8.2 statistical analysis system
- WebSphere MQ 6.0 queue manager
- EOS 1.4 report archive and distribution

13.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Operations Management Support Team
- DTS Enterprise Systems Team

14.0 Network Domain

14.1 Principles

The County is unique among its peers because it is its own telecommunications carrier. The County has undertaken several major initiatives to isolate itself from the uncertainty and expense of purchasing telecommunications services from the incumbent local exchange carrier (ILEC). Two major initiatives are the construction of a private facilities based electro-optical network (FiberNet I) and the installation of a large private branch exchange (PBX). These two initiatives have been complemented by two follow-on projects that leverage these investments. The first of these new initiatives was the installation of a metro-Ethernet network in 2007. This network is referred to as FiberNet II. The second initiative is the deployment of Voice over Internet Protocol (VoIP) as an alternative to digital wireline dial tone. These projects are well under way and very successful.

FiberNet is the name of the County's network. Based on economics and public safety concerns, the County can choose between FiberNet and the Local Exchange Carrier for telecommunications services and solutions. Telephony, public safety radio, data, secure Internet access, and video application services ride over FiberNet. From the County's perspective, FiberNet is a self-owned and operated electro-optical wide, campus, and local area network infrastructure, supplemented, when necessary, with ILEC frame-relay and TDM services.

The County built and manages its own network infrastructure. FiberNet is a robust and resilient service provider class network composed of over 500 miles of optical fiber plant, ATM and Ethernet switches, routers, one and ten Gigabit Ethernet (GbE) links and frame-relay circuits. These technologies are combined to deliver connectivity solutions that are efficient, bandwidth-rich, and economically justifiable. The first principles of engineering design are performance, security, reliability and availability, and these principles dominate FiberNet's daily operation. Cost recognition, reduction and containment are the economic principles that guide the operation of the network. FiberNet is monitored and evaluated against these principles and improved accordingly.

Montgomery County's network infrastructure supports a distributed user community, providing public safety and health services, traffic signal management, highly successful Internet-based eGovernment, back-office business applications, justice information systems and education.

FiberNet is a multi-agency telecommunications resource that is subject to inter-agency governance. FiberNet's strategic planning, budgeting and operational oversight is a matter of concern and involvement by the County Council which created the Information Technology Planning and Coordinating Committee (ITPCC) and its subgroups. This governance structure manages the direction of FiberNet, approves budgets and oversees the stewardship of DTS in operating the network.

FiberNet is a multi-service network infrastructure supporting voice, video and data to hundreds of sites within Montgomery County. The network has been operational for over eight years. New sites are added regularly.

FiberNet is currently undergoing an upgrade to a next-generation metropolitan area network technology based network called FiberNet II.

14.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the Network Services Team.

15.0 PBX Network Domain

15.1 Principles

The PBX Network Domain provides advanced voice services for most of the County Executive Branch Departments. The DTS PBX Telephone Services team provides the following services:

- Legacy Voice Services
- VoIP Services
- PhoneMail
- Manages the connection and agreement with the County ILEC
- Maintains the County Phone Directory – both online and printed

The County maintains a modern Avaya Communication Manager that leverages the Network Domain (see Chapter 14) to provide the above services. Communications Manager is a highly reliable and scalable system that provides access between voice and data endpoints.

The DTS PBX Telephone Services team supports both legacy voice and newer VoIP services. New installations are now being installed as VoIP services. The Communication Manager system supports both the old legacy voice and the newer VoIP services, enabling the County to continue to leverage its investment and allocate funds for new locations and new applications.

15.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Services Team.

16.0 Public Safety Domain

The Public Safety Domain supports the following departments:

- Montgomery County Police Department (MCPD)
- Fire and Rescue
- Sheriff's Office
- Department of Correction and Rehabilitation (DOCR)
- State's Attorneys Office (SAO)
- Circuit Court
- Department of Health and Human Services
- Department of Technology Services (DTS)

The domain has been moved from this document into its own Architectural Slice. The public safety domain is now documented in the Montgomery County Government Public Safety Information Technology Architecture.

The Public Safety Architectural slice includes the following architectural elements for the Public Safety Domain:

- Business
- Technical
- Data
- Application

17.0 Record and Document Management Domain

17.1 Principles

The Record and Document Management Domain is Montgomery County's integrated, comprehensive enterprise approach to centrally administer and manage all county electronic records.

The Records Management function for Montgomery County is the responsibility of the Department of General Services (DGS), Division of Operations Support Services Section. They own the responsibility for Records Management in the County which includes both physical and electronic records. They define the policy the county will follow, enforce the policy, provide education on the policy, define the tools (warehouse and IT) that will be used to implement the policy, etc.

Records Management is a management discipline that is responsible for the control of official records. It is a methodology for defining important records, their safe storage, how they can be used, how long they must be retained, and when they can be destroyed. A data retention policy is an important aspect to the Records Management function.

The DTS Core Systems team supports their IT Requirements by maintaining a Document Management/Imaging solution. The solution accommodates records from virtually any source, including scanned documents, electronic files (e.g. Microsoft Word, PDF, JPEG, etc), e-mails and attachments, COLD reports and other business applications.

Document Management/Imaging is part of the Records Management function and is the current tool used to support the Records Management domain. The Document Management/Imaging function will be integrated with Records Management once a more complete Records Management solution is identified.

DTS will maintain a Record and Document Management section on the DTS departmental homepage on the Intranet Portal. The Record and Document Management section will contain information about the service as well as an intake form and a roles and responsibility document. Finally, it will contain a directory listing for the electronic Records and Document management sites.

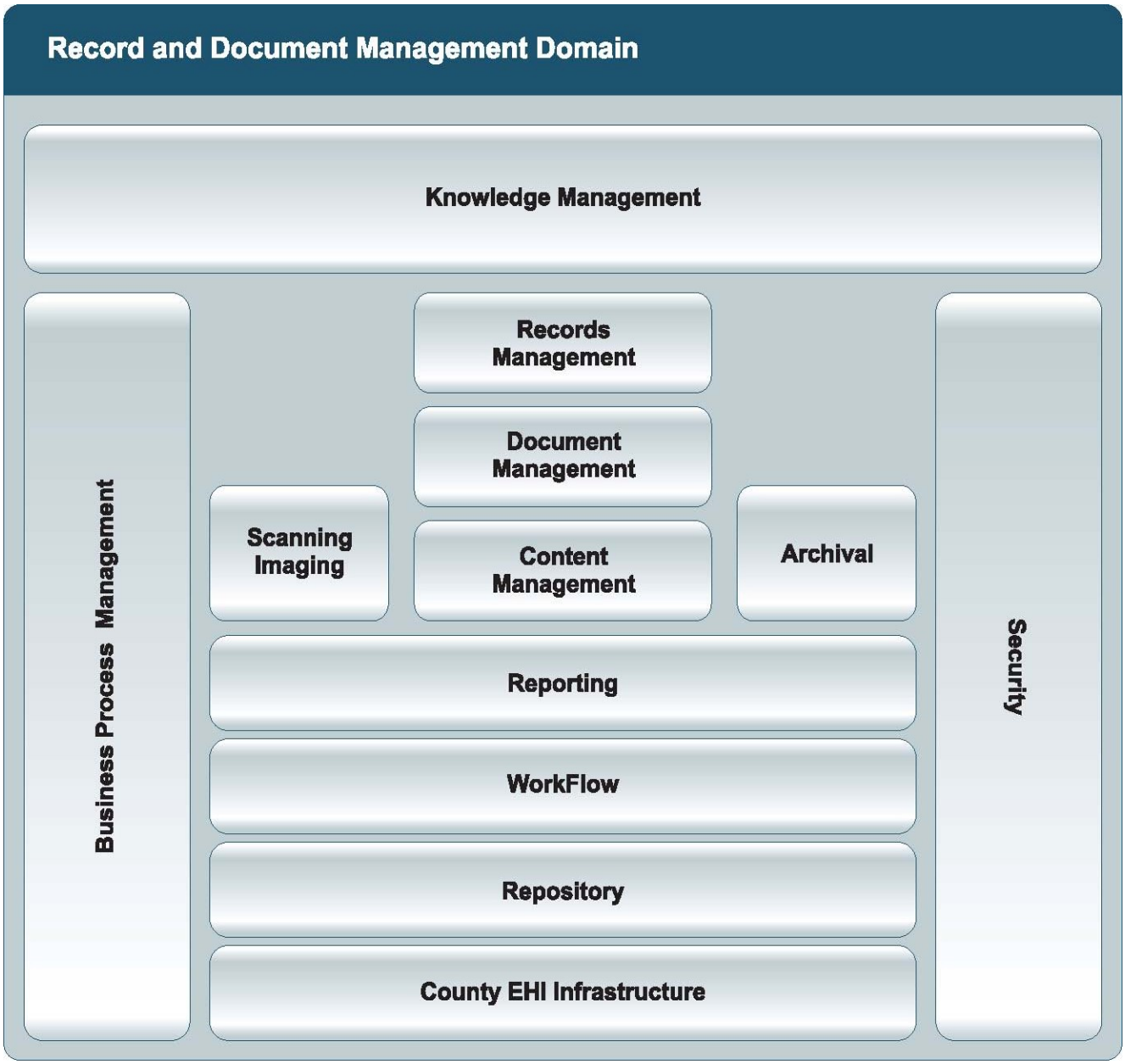


Figure 17-1 Records and Documents Management

17.2 Owners

Business Owner

The business owner for this Domain is DGS's Division of Operations Support Services Section.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

18.0 Reporting Domain

18.1 Principles

The County has two reporting packages to meet its diverse Enterprise Reporting requirements. The County uses SAS and Crystal Reports because each offers distinct capabilities and optimizes the use of software licenses.

18.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

19.0 Service Enabled Domain

19.1 Principles

The Service Enabled Domain promotes the development of robust, scalable and flexible services for business integration with the County infrastructure. The goal is to achieve a cooperative and secure service and data sharing environment, and to avoid data replication

The County recognizes the importance of developing Services capable of integration with internal and external systems. These Services will be designed and implemented, based on events and messages. An event-based, messaging model will help avoid stovepipes (rigid, self-contained functionally organized service solutions for each department, not acting as a single-entity). To do this, the County hosts a healthy mix of services. Some have been developed in-house, and some are COTS (Commercial Off-The-Shelf) solutions. Each application will document and publish well-defined interfaces to the protocols identified in this section.

An events-based messaging service will foster the maturation of service implementations based on Service Oriented Architecture (SOA). The County encourages the use of XML to define event messages, Web Services technologies for integrating .NET and J2EE services and Enterprise Java Bean (EJB) for integrating J2EE services. The following table lists the County's supported protocols.

Protocols
Message Q
Enterprise Java Bean (EJB)
Java Messaging Services (JMS)

Service Oriented Access Protocol (SOAP)
Secure Hypertext Transfer Protocol (HTTPS)
Web Services Description Language (WSDL)
Universal Description Discovery and Integration (UDDI)

Table 19-1 Service Enabled Domain Protocols

19.1.1 Enterprise Service Bus (ESB)

The County has deployed and maintains a distributed event services environment for communications between peer Services. This event service environment uses the SOA architecture pattern called Enterprise Service Bus (ESB). ESB is a specific server implementation of Service Enabled Domain services. ESB provides the feature capabilities listed in table 19-2.

Features
Protocol Switching
Message Routing
Message Transforms
Message Transports
Message Security
Message Aggregation/Splitting

Table 19-2 ESB Feature Capabilities

ESB provides a rich, event-based messaging infrastructure that aids the implementation of complex Service Enabled Domain Services and client consumers. Figure 19-1 shows a modular overview of the ESB.

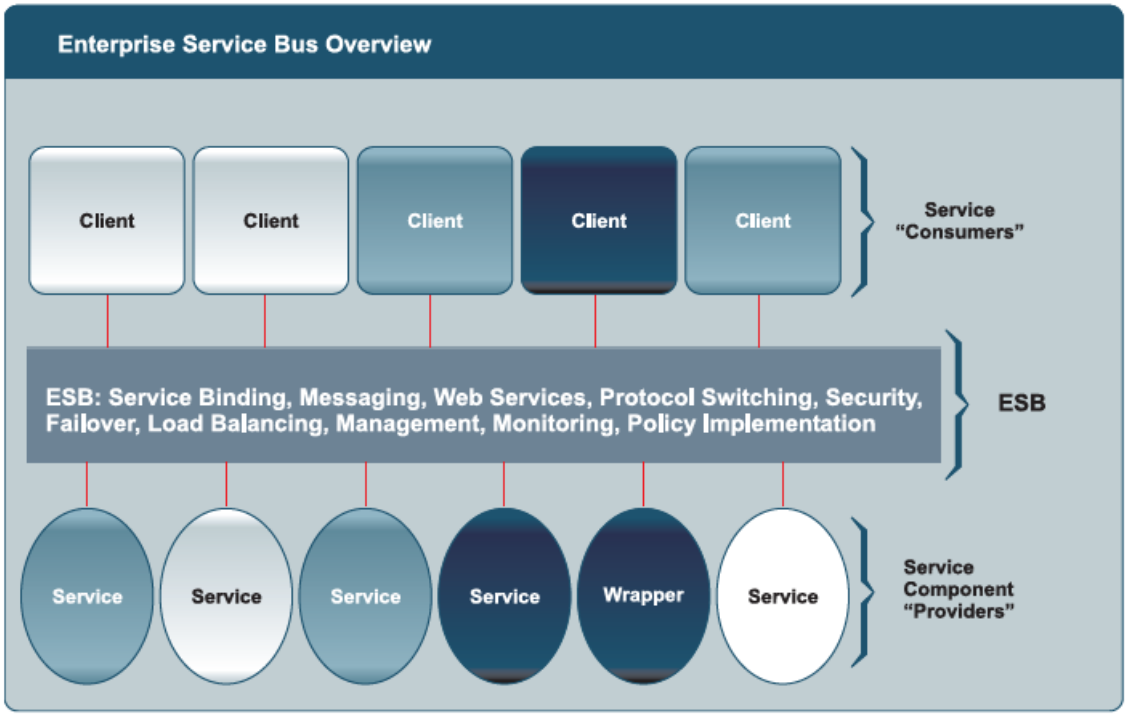


Figure 19-1 Enterprise Service Bus Overview

Compared to a home-grown Service Enabled Domain hosting environment, the standards-based ESB provides extreme flexibility for future integrations and extensibility. Figure 19-2 shows a list of comparison between classical Service platforms and ESB.

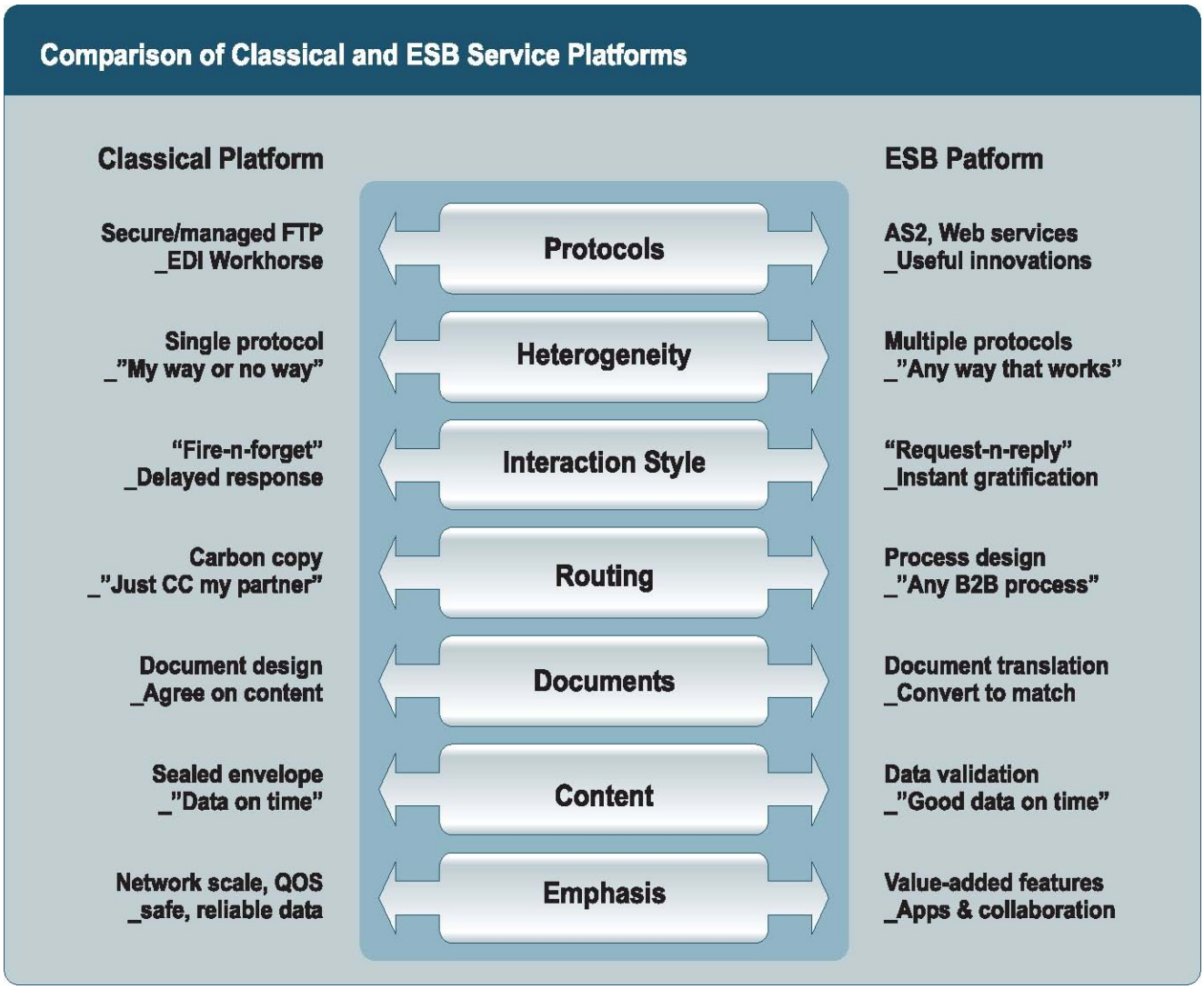


Figure 19-2 Classical vs. ESB Service Platforms

19.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

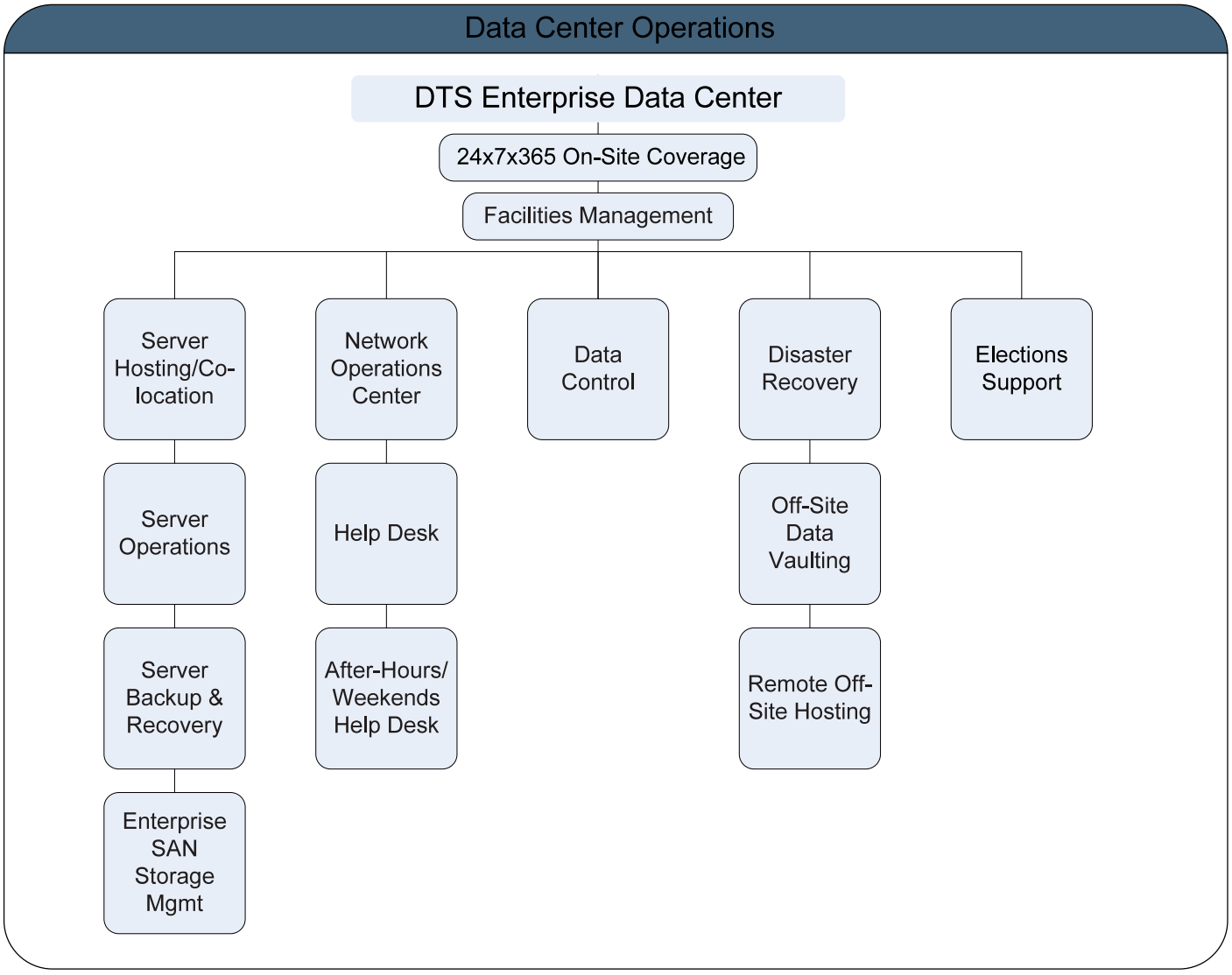
Technical Owner

The technical owner for this Domain is the DTS Enterprise Services Architect.

20.0 System Operations Domain

20.1 Principles

Data Center Operations provides first-line operational support and security (24-hours per day, 7-days a week) for mission critical servers, mainframe and main network hubs that reside in the County's Enterprise Data Centers. Major support services provided by the team include mainframe, server and Storage Area Network (SAN) operations, server backup/recovery, server hosting and system/network monitoring (NOC), Help Desk, including all after-hour calls and Data Production Control. Data Center Operations coordinates the Disaster Recovery plans and test exercises for several of the County's mission-critical systems. Operations maintains 3 shifts of staff on-site 24x7, while protecting the secured Data Center environments around the clock from power outages with UPS units and diesel generators. A constant climate controlled environment for the Data Centers is provided as well as fire protection and suppression systems. All hardware equipment is housed on a raised floor.



20.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Data Center Operations Team.

21.0 Web Application Domain

21.1 Principles

The County uses custom Web applications to meet the day-to-day requirements of an individual or an organization. It distinguishes these applications from Enterprise applications, which affect the County's core services. The Web Applications Domain addresses browser-based custom applications built with tools available on desktop operating systems. Generally, web applications are developed using Microsoft's .NET Framework or Active Server Page (ASP) technology. They use services of the County infrastructure for reliable sources of data.

Web Applications are developed to meet IT requirements local to an organization. Typically, they are short-cycle products, developed to meet tight deadlines with limited resources. On the other hand, Enterprise applications are strategic in nature, enabling County business processes and often available as Services. Figure 21-1 attempts to clarify Enterprise and Web application space.

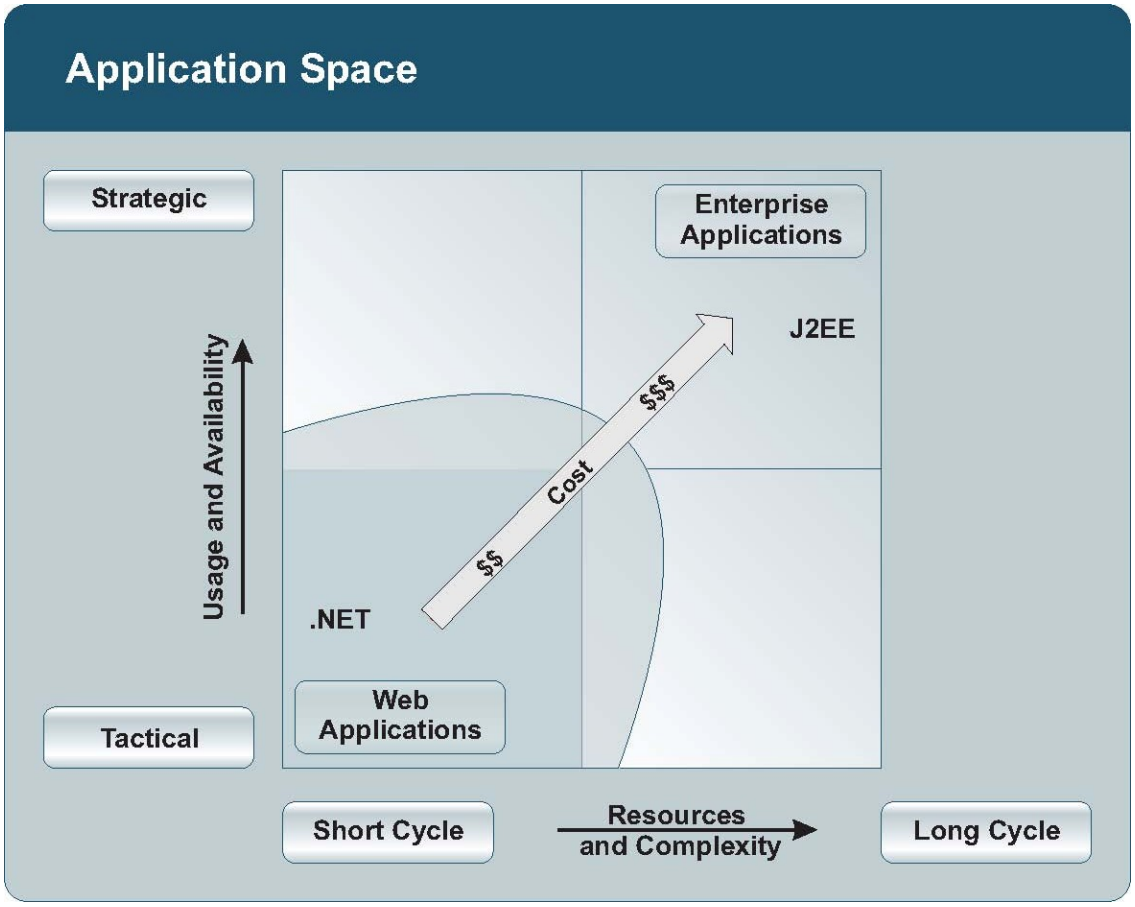


Figure 21-1 Enterprise and Web Application Space

21.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Application Development and Integration Team.

22.0 Team Collaboration

22.1 Principles

The Team Collaboration Service provides an easy to use online meeting place for internal county teams. Team members can come to a team portal and collaborate on projects using their desktop browsers. The collaboration service provides some of the following abilities to a team:

- Announcements
- Meeting Agendas
- Document Sharing
- Calendar
- Tasks
- Discussion Board
- Linking Ability

22.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

23.0 Configuration Management (CM) Tools

23.1 Principles

The Configuration Management Tools Service provides the following functions to a team:

- Version Control Code Repository
- Version Control Document Repository
- Requirements Tracking
- Bug Tracking
- Issues Tracking

23.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team.

24.0 Enterprise Server Management

24.1 Principles

The Enterprise Server Management Service provides the following functions for management of both physical and virtualized Enterprise Servers:

- Availability Monitoring
- Inventory Management
- Configuration Auditing
- Performance Monitoring
- Event Management
- Historical Data Tracking and Reporting
- Incident Alerts and Escalations

24.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team.

25.0 Software as a Service (SaaS)

25.1 Principles

The SaaS Domain supports the use of externally hosted applications by Montgomery County. This service provides support that solves the common issues around using an externally hosted application. The common issues that are addressed within the SaaS support are related to:

- Identity
- Security
- Integration

25.2 Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Enterprise Services Architect.

26.0 Web Portal Domain

Montgomery County supports both an Internet and Intranet Web Portal. The primary Internet Portal (www.montgomerycountymd.gov) is the main Internet (public access) entry point for County electronic government (eGovernment) services. The primary Intranet Portal (portal.mcgov.org) provides eGovernment services for County employees and associates (contractors, volunteers, partners, etc).

Montgomery County takes a decentralized approach to managing its web site. A small number of staff within the Department of Technology Services (DTS) and the Public Information Office (PIO) has responsibility for branding, information architecture, development of the centralized web content management system, navigational flow and development and oversight of web policies and procedures.

County Departments, Offices, and affiliated government agencies are responsible for the development of their own web content and applications. They are led by the following County Executive Branch groups:

- Public Information Office (PIO)
- DTS Application Development and Integration Team (DTS-ADT)
- DTS Server Team

The PIO, in partnership with DTS, reviews and recommends Internet and Intranet policy, standards, and practices to County Management for implementation on the County portals. DTS, typically in partnership with PIO, is primarily responsible for reviewing and enforcing County Intranet Portal policies.

The PIO, in partnership with DTS;

- reviews and approves virtual directory requests (shortcut policy) from County Executive Branch departments,
- enforces the County Internet URL and Standard Design Template Policy,
- develops, maintains, and updates the standard web portal template designs as well as the information architecture for the Internet Portal Domain, and
- develops and recommends for approval by County Management, the standards, practices and guidelines for:
    - privacy and user rights issues including linking from and to the County website,
    - web accessibility for residents with disabilities, and
    - web 2.0 (social networking) activities.

In addition, the PIO maintains and manages web content for primary Internet Portal web pages, including the County Home page.

The DTS-ADT provides application development and content management services, for customers including County Executive Branch Departments, boards, committees, and commissions, the County Council, and other affiliated County government agencies, such as the Circuit Court and the States Attorneys Office.

The DTS Server Team maintains the Intranet and Internet (MCGOV) Web Portal Domains including County Web and Application Servers, Streaming and Encoding Servers (MCGOV-only), Search Engine (Google) Servers, and Map Servers. In addition, the Server Team provides Intranet and Internet Server load balancing, incident response, and middleware support. Furthermore, the Server Team enforces access to the Web Portal Domains. File transfer access (read/write) permissions to the Web Portals are available through the County Content Management System (CMS) for web content and through JFM and/or an equivalent DTS approved tool for web applications.

While most County web content and web applications are hosted or stored on the Portal Servers, some departments (i.e. Department of Permitting Services, Department of Homeland Security and Emergency Management, and Department of Technology Services) own secondary web servers that are linked to and from the primary Portals. Secondary web servers are typically supported by the owning departments or offices and are approved by the PIO and DTS.

The Internet and Intranet Portals can support various types of web content files, application programming languages and technologies, and multimedia file formats including, but not limited to the following:

Programming Languages and Technologies

- Adobe Shockwave Flash (SWF)
    - ActionScript
- Dynamic Hyper Text Mark-up Language (DHTML)
    - HTML, Javascript, and Cascading Style Sheets (CSS)
- Extensible Hyper Text Mark-up Language (XHTML)
- Extensible Mark-up Language (XML)
- Extensible Stylesheet Language Transformations (XSLT)
- Hyper Text Mark-up Language (HTML)
- JAVA (see Chapter 8 - Enterprise Applications Domain)
- Keyhole Markup Language (KML)
    - KML is used to specify a set of geo-spatial features (placemarks, images, polygons, 3D models, textual descriptions, etc.) for display in Google Earth, Maps and Mobile, or any other 3D earth browser (geo-browser) implementing the KML encoding
    - Typically compressed in Keyhole Markup Zip (KMZ) files

- Microsoft Active Server Pages (ASP)
- Microsoft Active Server Pages.NET (ASP.NET)
- Really Simple Syndication (RSS) 2.0
- Synchronized Multimedia Integration Language (SMIL or SMI)

Multimedia Files

- Adobe Flash Video (FLV)
- Adobe Shockwave Flash (SWF)
- Microsoft Windows Media Audio (WMA)
- Microsoft Windows Media Video (WMV)
- Moving Picture Experts Group - Layer 3 (MP3)

Web Content Files – Static

- Adobe Portable Document Format (PDF)
- Graphics Interchange Format (GIF) – Image File Format
- Hyper Text Mark-up Language (HTML)
- Joint Photographic Experts Group (JPG) - Image File Format
- Microsoft Active Server Pages (ASP)
    - Used as the County's primary web content file format
    - Primarily consists of HTML
- Microsoft Office Files
    - PowerPoint (PPT), Excel (XLS), or Word (DOC, RTF, or TXT)
- Portable Network Graphics (PNG) – Image File Format
- Synchronized Multimedia Integration Language (SMIL or SMI)
- WinZip Files (ZIP)
    - Used to compress files for faster download speeds

The Web Portal Domain provides accessible web content and rich web applications featuring the following technologies:

- Web 2.0
    - County Information Center web applications enables users to subscribe to Really Simple Syndication (RSS) feeds and on-line newsletters, to read and interact with County Blogs, and to engage County leaders in on-line discussions
    - County On-Demand web applications provide access to web content (i.e. videos, news releases, etc..) using YouTube, Twitter, and Facebook technology
    - The Alert Montgomery System enables users to register to receive emergency alert text messages and notifications
    - MyMontgomery, an on-line mapping application integrated with Google Maps, enables users to find County service locations or places of interest (PLOI) by street address and zip code or by zip code only
- Web Accessibility
    - A dynamic text-only conversion function built into County Portal web site templates enables screen reader browsers and other assistive technologies to access County web content (static)
    - A language translation web application uses Google's machine language translation tools to dynamically convert County web content into Spanish/Hispanic, Chinese, French, Korean and Vietnamese languages
    - A screen reader software (*BrowseAloud*) helps users with low literacy and reading skills, limited English proficiency, dyslexia or related disabilities, or mild visual impairments to access County Internet web pages

    - Voice recognition technology is linked with selected human resources web applications County employees
- Web Content Discovery and Management
    - A semantic – friendly County Services Center web application / database is integrated with Google Mini Search Appliance technology to enable users to quickly find on-line County services and information by keyword or phrase
    - A Content Management System is used to maintain and manage County Web Portal (Internet and Intranet) web content. Content providers are trained and encouraged to use descriptive links and page titles to improve content discovery

26.2 Owners

Business Owner

The business owner for this Domain is the Public Information Office.

Technical Owner

The technical owners for this Domain are:

- DTS Application Development and Integration Team
- DTS Server Team
- Public Information Office

26.3 Internet (MCGOV) Web Portal Domain

26.3.1 Principles

The audience for the Internet Portal includes, but is not limited to the following:

- County Residents and Visitors
- Other Government entities
- Business owners and operators
- Job seekers
- Other constituents

The publicly accessible web applications and content deployed on MCGOV Servers generally support the following functions:

1. Data Collection
    a. Recording or capturing data from constituents (i.e. registration for a meeting, survey, etc…)
    b. Enabling constituents to report an incident, event, etc… (i.e. pothole, street light outage, etc…)
2. Information Referral
    a. General query, results, and details information referral applications
    b. Interactive maps and travel directions (ArcGIS and Google map services)
    c. Multimedia streams (video and audio)
    d. Static web pages providing information referral services
    e. Web Services (i.e. street address validation)
3. On-line Payment Transactions
    a. Automated Clearinghouse (ACH) – On-line Check Payments (NACHA compliant)
    b. Credit Card Payments
4. Subscriptions, Blogs, Interactive Messaging
    a. On-line newsletter and RSS feed subscriptions
    b. Blogs (Read-only)
    c. Message Boards (Live Discussion)
    d. Messaging (Emergency Alerts)

26.4 Intranet Portal

26.4.1 Principles

The function of the Intranet portal is to support:

- Employee communications
- Employee services
- Departmental pages

The audience for the Intranet portal includes:

- Employees, Paid Interns, Temporary Workers (Active)
- Associates (Active)
  - Contractors
  - Partners - affiliated company/business user accounts, partners to the County
  - Volunteers - Volunteers, unpaid Interns

Appendix A Data Architecture

Introduction

Montgomery County leverages Information Technology to sustain its operational and strategic decisions support systems. All key information systems store, manage, and use data to predict, model, and control the flow of information in the system. It is a challenge among data modelers to identify best practices in data definition and design.

Data Architecture creates a logical data model for the County's Lines of Business (LOB) and is designed to promote common vocabulary and data definition.

The guiding principles for the Data Architecture are:

Data is an asset, accessible and shared for decision support and interoperability
Data is secure, and protected from unauthorized use and disclosure
Data is stored and accessible with technology independent methods
Data has an owner and an established system of record

Purpose

The purpose of the Data Architecture is to build a platform which will enable rapid development of distributed, multi-tiered applications. The purpose of this section is to identify the County's common data structures in XML or database schema definition, and to associate those data structures to their source platforms. Application Program Managers and Developers are encouraged to use this authoritative information in their design and development efforts.

This Data Architecture will enable the development of flexible, adaptable and stable applications, facilitate rapid information sharing across the County, and enhance and accelerate decision making. This section provides data standards for enterprise applications and COTS systems, which will be a guide for integration and business process re-engineering. The County's data architecture supports information-centric data exchange mechanisms. By promoting secure services for data exchange, it will enhance end-user computing. With this model, the County will improve data integrity among distributed applications. The following figure represents data modeling along Lines of Business (LoB), as discussed above.

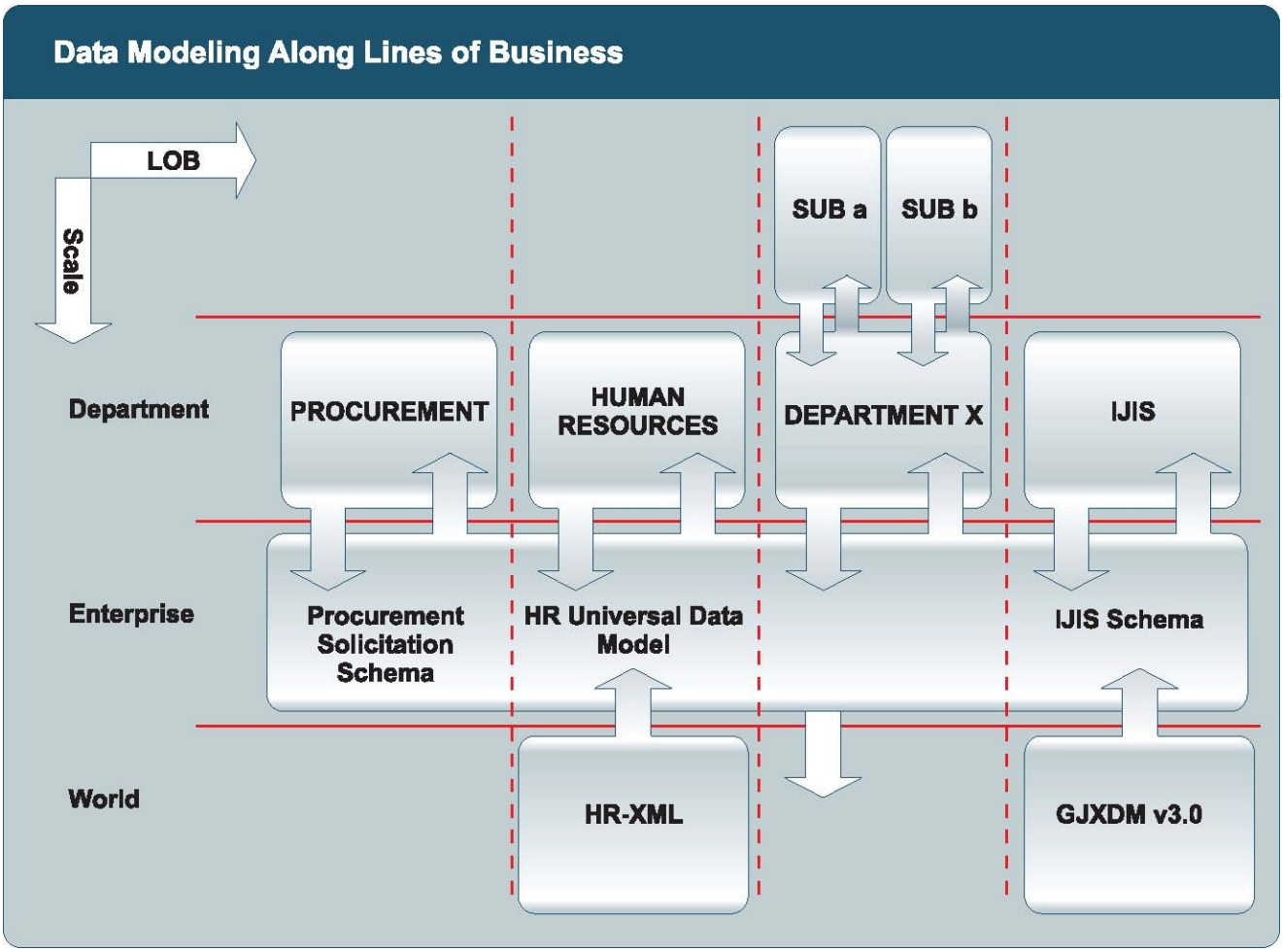


Figure B-1 Data Modeling along Lines of Business

Functional requirements are important because they define and drive the data requirements. Data is used to:

- Complete transactions, short and long-lived
- Develop detailed and roll-up reports for decision-making
- Execute dynamic queries and generate ad-hoc reports
- Develop a data warehouse for coherent business analysis

Data architecture is an essential component of information technology architecture. It is intrinsic in developing successful service-oriented architecture. A comprehensive data model of information, along LoB, facilitates rapid development of coherent departmental and enterprise business applications. It provides guidance in developing enterprise application integration (EAI) and enterprise information integration (EII) strategies.

Appendix B Contractor's Resource Kit

B-1.0 Background

Montgomery County Government has adopted the Project Management Body of Knowledge (PMBOK), created and endorsed by the Project Management Institute (PMI) as the accepted standard for Project Management for all of the County Projects. A Project Management Methodology has been built around this standard, and vendors are required to incorporate this methodology into the Vendor preferred project management methodology proposed in any RFP or negotiated contract.

In recent procurements the County has realized that each vendor comes with their own Project Management Methodology, which may or may not, meet County expectations. Based on this, the County will now require all vendors to review this document, and adopt the County Project Management Methodology and Standards, or map their process, deliverables, and standards to comply with the minimum County Standards. The following document provides a description of the methodology, the deliverables, and a checklist for those deliverables.

Vendors are free to propose their own templates, if those templates include the items of the County standards checklist. The vendor templates must be reviewed and approved by the County Project Manager assigned to the project as part of the overall project plan. The County's preferred templates are appended to this document.

B-2.0 Project Management Methodology

The Montgomery County Government's Department of Technology Services (DTS) has a series of project phases and Quality Checkpoints built in to a Project Management Framework. The six phases of the project methodology are listed below with a bulleted listing of the deliverables supplied by the County and those that will be expected from a vendor. A description of each deliverable/document is included in this document, as well as the expected role of the vendor's Project Team for that deliverable. Each deliverable described below also contains a checklist of the items needed to meet County expectations for the vendor to receive signoff from County personnel.

B-2.1 Phases/Key Deliverables

There are six phases containing Key Deliverables unique to each phase.

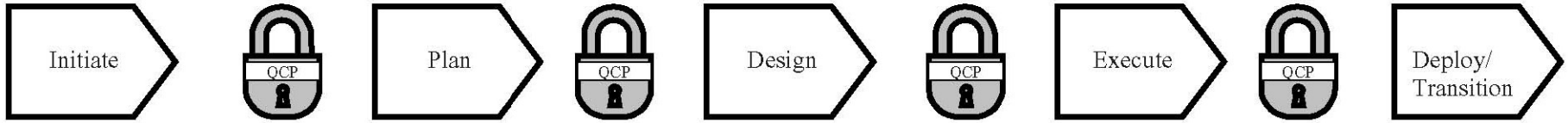
- Initiate
- Plan
- Design
- Execute
- Deploy
- Control

B-2.2 Quality Check Points

At the end of each project phase, a Quality Check Point meeting will be held with the Project Team to

ensure that all deliverables are acceptable, and that they have been approved by the County Project Team. An assessment of the Project Plan will be done and updates/changes will be made.

Montgomery County Government Project Management Framework/Key Deliverables
External Vendor Toolkit



Provided by County
- Project Sponsor Sign off
- Business Case
- Cost/Benefit Analysis
- Steering Committee
- Work Group/Core Team
- Preliminary Project Requirements
- Preliminary Traceability Matrix
- Funding Source
- Project Manager
- Project Performance Criteria
- Stakeholder Identification List

Vendor Deliverables
- **Statement of Work**
- **Project Charter**
- **Vendor Team**
- **Performance Measures**
- **Preliminary Project Plan**
- **Communication Plan**
- **Quality Plan**
- **Implementation Strategy**
- **High Level Project Schedule Proposal**
- **Project Kick off Meeting**

Quality Check Point

Provided by County
- Assign Budget/Contract Manager
- Assign Subject Matter Experts
- Assign Project Team Leads
- Change Control Plan
- Change Control Board

Vendor Deliverables
- **Process Flows**
  - **"As is" Process Flows**
  - **"To be" Process Flows**
  - **Gap Analysis**
- **Final Business Requirements Sign off**
- **Final Technical Requirements Sign off**
- **Project Plan**
- **Risk/Contingency Plan**
- **Preliminary Implementation Plan**
- **Preliminary Training Plan**
- **Preliminary Architecture and Design Plan**
- **Preliminary Operational Readiness Plan**
- **Procurement Plan**
- **Testing Plan**
- **Change Management Plan**

Quality Check Point

Provided by County
- Legacy System Architecture
- Database Specs County sys
- Existing Network Diagrams
- Existing Infrastructure
- County Architecture Standards
- Existing Interfaces

Vendor Deliverables
- **Architecture Document**
- **Design Document**
- **Interface/Integration Design Document**
- **Functional Design Document**
- **Data Conversion Plan**
- **Configuration Management Plan**
- **Training Plan**
- **Testing Plan**
- **Test Scripts**
- **Traceability Matrix**
- **Work Breakdown Structure**
- **Baseline Project Plan**
- **Operational Readiness Plan**
- **Implementation Plan**

Quality Check Point

Provided by County
- Subteam Formation
- Work Packet Deliverables
- Data Conversion preparation
- Integration Testing Participate
- System Testing Participation
- Configuration Participation
- Test Environment
- Training Plan execution
- Operational Readiness Preparation
- User Acceptance Testing Participation
- Disaster Testing County Participation

Vendor Deliverables
- **Work Packet Deliverables**
- **Test Environment**
- **Unit Testing**
- **Integration Testing**
- **System Testing**
- **UAT**
- **Configuration Management/ documentation**
- **Data Conversion**
- **Disaster/Recovery Testing**
- **Training Manual/Web based modules**

Quality Check Point

Provided by County
- Implementation Support
- Post Implementation support plan
- Ongoing Training Support
- Operations Plan
- Transition Plan
- Implement Performance Measures
- Project Close Out
- Service Level Agreement

Vendor Deliverables
- **Production Environment**
- **Implementation**
- **Implementation Validation**
- **Post Implementation Support Plan**
- **Disaster/Recovery Manuals**
- **Configuration Management Process Manuals**
- **Operations Manual**

Project Closeout

Control

Provided by County
- Status Reports
- Critical Path Reports
- Weekly Project Plan updates
- Contingency Planning
- Project Audits
- UAT Reports

Vendor Deliverables
- **Risk Assessment**
- **Critical Path Monitor and Report**
- **Operational Readiness Assessment**
- **Continuity of Business Plan**
- **Performance Measurement Report**
- **Traceability Matrix test results confirmed**
- **Status Reports Weekly Project Plan Updates**
- **Risk Matrix**
- **Issues Tracking**
- **Testing Reports**

Control

B-3.0 Phase 1 – Project Initiation

When an RFP is issued, several of the phase 1 deliverables have been completed by the County Project Initiation team. The project initiation and prioritization process for IT projects requires a project sponsor. This project sponsor will approve and submit a solid business case, cost/benefit analysis, and Statement of Work to the Department of Technology Services. Requests are reviewed and rated by the DTS team. When they have been judged ready for consideration, the requests are submitted to the annual budget process to receive funding. If a department has been granted funding, it will be assigned both business and technical representation to complete the Request for Proposal (RFP). The County will have received Sponsor sign off on the project charter, and will have agreed on the scope of services to be addressed in an RFP.

B-3.1 Statement of Work

B-3.2 Project Charter

A Project Charter should be jointly developed between the County Project Manager(s) and the Vendor Project Manager. This document must list the roles and responsibilities of the project team's groups, and identify the structure of the project team. This document shall be used as input to the overall Project Plan. The County has a standard Governance Template that it prefers to use, but it will consider modifications based on project variables. The Project Governance Document must include:

- Project structure's functional departments
- Project structure's technical divisions
- Project structure's Vendor teams by as defined by function
- Project function's list of required project team leaders
- County Project Manager(s) (Projects may include functional as well as a technical Project Manager)
- Vendor Project Manager
- Workgroup
- Contract Administrator
- Project Administrative support
- Steering Committee
- Change Control Board

B-3.3 Vendor Team

B-3.4 Performance Measures

B-3.5 Preliminary Project Plan

Once the RFP and the negotiations are completed, there will be a defined and contracted scope of services/work. This scope should be used to create a project plan. In the start up phase of the project, vendor resources should work with County Project Manager(s) to:

- Review and understand the scope of work
- Identify all County and non-County Stakeholders
- Identify the known issues, assumptions and constraints
- Review any relevant policies, laws, or federal mandates affecting the project

- Review historical information from past projects
- Estimate required resources from functional and technical areas

The Vendor Project Manager will work with the County Project Manager(s) to create a preliminary plan to control and manage execution of the project. The project plan will be a document that continues to be defined and refined through the life of the project as new details become available. The preliminary project plan will include a minimum of the following:

- Project Charter
- Project Governance Chart
- Scope Statement, which includes the project deliverables and the project objectives
- Performance measurement baselines for schedule and cost
- Major Milestones and target dates for each deliverable
- Key Staff/Resources

Description of the project management approach or strategy
This would be a summary of the plans to be developed and described in later phases.
Risk Plan addressing major risks, constraints and assumptions and their planned responses

- Open issues and pending decisions
- Communication Plan
- Quality Assurance Plan
- Test Plan
- Change Management Plan/Scope Management Plan
- Operational Readiness/Change Management Plan
- Implementation Plan

Project Schedule
The County uses Microsoft Project as the standard tool.

- Work Breakdown Structure (WBS) with the levels at which control will be exercised
- Cost Estimates by Work Package, if applicable
- Scheduled start dates for the WBS work packages
- Duration Estimates
- Resource Requirements
- Dependencies
- Critical Path Calculations

B-3.6 Communications Plan

B-3.7 Quality Plan

B-3.8 Implementation Strategy

B-3.9 High Level Project Schedule Proposal

Project Schedule

- The County uses Microsoft Project as the standard tool.
- Work Breakdown Structure (WBS) with the levels at which control will be exercised
- Cost Estimates by Work Package, if applicable
- Scheduled start dates and end dates for the WBS work packages
- Duration Estimates

- Milestones
- Resource Requirements
- Dependencies
- Critical Path Calculations

B-3.10 Project Kick-off Meeting

The purpose of the project's Kick Off Meeting is to introduce the County's Stakeholders to the principal County Project personnel, and to introduce the project. The vendor will present an overview of their company, an overview of the project, its intent, purpose, stakeholder identification, and project approach and timeline. If the project involves a COTS product, the vendor should arrange a demonstration of the product. With a minimum of two weeks notice, the county will work with the vendor to schedule the Kick Off Meeting.

B-3.11 Project Governance Document

B-3.12 Requirements ID

There are two types of requirements documents. One is a requirements matrix with a scope of services description in the RFP, and the other is a requirements matrix from the scope of services.

If a requirements Matrix has been provided, you will use the Process Mapping technique to revalidate the requirements and verify the scope of work. Additional requirements not identified in the requirements matrix will be documented, as will requirements in the matrix found to be no longer needed. A gap document will be prepared, and the Change Management process will be followed, as identified in the Project Plan.

To review the scope of services in the RFP and to create the Requirements Matrix, use the process mapping techniques described in this document. This will identify the requirements and put them into the county standard Requirements Matrix Format. All of the requirements documents will require sign offs from the project leads, the County Project Manager(s), and the Project Sponsor.

B-3.13 Process Maps

"As Is" -The vendor will map the current "as is" state of the business, or revalidate a previous "as is" process map. These maps will be detailed enough to capture the entire business process from beginning to end for the addressed services. All processes, both manual and systemic, interface points, roles and responsibilities, and actions will be documented.

The Process Map is to be done by the vendor's staff using on-the-job observation, interviews, Subject Matter Experts (SME) JAD sessions and supporting documentation. These observations, interviews, JAD session results, and documents will be captured in an electronic process flow format. Visio is the County process map tool of choice. If a vendor chooses to use another tool, it must be supplied at the vendor's expense, to the county personnel responsible for reviewing and validating the process flows. The vendor must hold JAD sessions with County staff subject matter experts to review and confirm the accuracy of the 'As is" process flows, and to obtain sign offs from the appropriate project leads and the County Project Manager.

"To Be" –The vendor will map the "To Be" state of the business based on requirements from the scope of service, the requirements matrix, and the discovery process the "As Is" processes. It is the vendor's responsibility to identify the opportunities for process improvement within the requirements for the "to be"

process flows. Visio is the County's current process map tool. If a vendor chooses to use another tool, it must be made available at the vendor's expense to county users responsible for reviewing and validating the process flow. The vendor must hold JAD sessions with County staff SMEs to confirm the 'To Be" process flows, and to obtain sign off from the appropriate project leads and the County Project Manager.

Gap Analysis/Operational Change Assessment – Once the "As Is" and "To Be" process flows have been completed, and the sign off approval has been granted, it is the responsibility of the Vendor to hold JAD sessions with the SMEs. The sessions will document the gaps or process changes that will need to be covered in the Operational Readiness Plan. These gaps will be addressed in Training Documentation, issues logs, action items, and the risk log. In the planning phase, these will move into the Operational Readiness Plan.

Architecture document

This section will document a checklist of submissions by a Contractor or Development Manager for product architecture.
The content will include:

1. Application Process View
2. Deployment and Network View
3. Integration and Interface View
4. Security View
5. User Interface View
6. Compliance View

Design document

This section will document submissions for product design.
The content will include:
System Design for:

1. Scalability
2. Availability
3. Reliability
4. Technical Feasibility
5. Support and Assurance
6. Standards
7. Performance
8. Design Patterns

Integration document

This section documents submissions by a Contractor or Development Manager for product integration capabilities.
The content will include:

1. Interface design
2. Platform design
3. Exception and error handling/recovery guide
4. Operations guide
5. Service Level Agreement (SLA)

Quality Assurance document

This section will document a checklist of submissions by a Contractor or Development Manager on QA practices.
Content will encompass:
QA strategy for:

1. Development
2. Systems
3. Integration

Defect document

This section will document a checklist of submissions by a Contractor or Development Manager on recording and managing product defects.

Content will encompass:

1. Defect recording
2. Defect processing
3. Communication practices

Deployment document

This section will document a checklist of submissions by a Contractor or Development Manager on product deployment.

Content will encompass:

1. Systems packaging
2. Systems requirements
3. Application setup/configuration
4. Maintenance

Change Request document

This section will document a checklist of submissions by a Contractor or Development Manager on identifying, recording and managing changes to the product.

Content will encompass:

1. Identifying, recording and processing change requests
2. Communication practices

Appendix C Application Security Standards

The County makes use of the following security standards for implementing applications:

a. Parameter Tampering Prevention - ensure that all parameters are validated before they are used. Parameters should be validated against a “positive” specification that defines:
   - Data type (string, integer, real, etc…)
   - Allowed character set
   - Minimum and maximum length
   - Whether null is allowed
   - Whether the parameter is required or not
   - Numeric range
   - Specific legal values (enumeration)
   - Specific patterns (regular expressions)

b. Access Control or Authorization Standards - Access control and authorization standards are based on the Single Sign On (SSO) architecture the County has implemented. The County uses SSO to do both authentication and authorization. In general, the rules and authorization are defined. When developing an application, the most important step is to think through an applications’ access control matrix to define the access control rules. Without documenting the security policy, there is no definition of what it means to be secure for that site. The policy should document what types of users that can access the system and what functions and content each of these types of users should be allowed to access. The access control mechanism should be extensively tested to be sure that there is not way to bypass it. This testing requires a variety of accounts and extensive attempts to access unauthorized content or functions. Some specific examples of access control issues include:
   - Insecure Id’s (application side)
   - Forced Browser Past Access Control Checks (application side)
   - Path Traversal (server side)
   - File permissions (server side)
   - Client Side Caching **–** Developers should use multiple mechanisms, including HTTP headers and meta tags, to be sure that pages containing sensitive information are not cached by user’s browsers.

c. Broken Authentication and Session Management - Browser Caching **–** Authentication and session data should never be submitted as part of a GET, POST should always be used instead. A session should only be created after authentication. Authentication pages should be marked with all varieties of the no cache tag to prevent someone from using the back button in a user’s browser to backup to the login page and resubmit the previously typed in credentials. Many browsers now support the autocomplete=false flag to prevent storing of credentials in autocomplete caches.

d. Cross-Site Scripting (XSS) Flaws - To protect a web application from XSS attacks is ensure that the application performs validation of all headers, cookies, query strings, form fields, and hidden fields,(i.e., all parameters) against a rigorous specification of what should be allowed. The validation should not attempt to identify active content and remove, filter, or sanitize it. There are too many types of active content and too many ways of encoding it to get around filters for such content. A ‘positive’ security policy that specifies what is allowed. ‘Negative’ or attack signature based policies are difficult to maintain and are likely to be incomplete. Encoding users supplied output can also defeat XSS vulnerabilities by preventing inserted scripts from being transmitted to users in an executable form. Applications can gain significant protection from JavaScript based attacks by converting the following characters in all generated output to the appropriate HTML entity encoding:

From:	To:
<	&lt;
>	&gt;
(	&#40
)	&#41
#	&#35
&	&#38

e. Buffer Overflows - For custom application code, review all code that accepts input from users via the HTTP request and ensure that it provides appropriate size checking on all such inputs. This should be done even for environments that are not susceptible to such attacks as overly large inputs that are uncaught may still cause denial of service or other operational problems.

f. Injection Flaws - The simplest way to protect against injection is to avoid accessing external interpreters wherever possible. For many shell commands and some system calls, there are language specific libraries that perform the same functions. Using such libraries does not involve the operating system shell interpreter, and therefore avoids a large number of problems with shell commands.

   For those calls that must still be employed, such as calls to backend databases; carefully validate the data provided to ensure that it does not contain any malicious content. Search criteria are supposed to be for data and not an executable statement. Structure many requests in a manner that ensures all supplied parameters are treated as data, rather than potentially executable content. The use of stored procedures or prepared statements will provide significant protection, ensuring that supplied input is treated as data. These measures will reduce, but not completely eliminate the risk involved in these external calls. Always validate such input to make sure it meets the expectations of the application in question.

   All output, return codes and error codes from the call should be checked to ensure that the expected processing actually occurred. At a minimum, this will allow one to determine that something has gone wrong. Otherwise, the attack may occur and never be detected.

g. Improper Error Handling – When errors occur, the site should respond with a specifically designed result that is helpful to the user without revealing unnecessary internal details. Log certain classes of errors to help detect implementation flaws in the site and/or hacking attempts.

h. Denial of Service – For unauthenticated users, avoid any unnecessary access to databases or other expensive resources. Architect the flow of the site so that an unauthenticated user will not be able to invoke any expensive operations. Consider caching the content received by unauthenticated users instead of generating it or accessing databases to retrieve it. Check the error handling scheme to ensure that an error cannot affect the overall operation of the application.

Appendix D Coding Standards

The purpose of these guidelines is to provide a coding standard for software developers. By following the guidelines, software developers can create code that is easier to read, easier to understand, and easier to maintain. This document applies to all members of the development team and should be referenced on all software development. Everyone should read, understand, and use them. These standards will evolve as Java and .NET are implemented into the County's IT Architecture.

Naming Conventions

General Conventions

- Use full English descriptors
- Use terminology applicable to the domain.
- Use mixed case to make names readable.
- Use abbreviations sparingly, but if you do so then use them intelligently.
- Avoid long names (< 15 characters is a good idea).
- Avoid names that are similar or differ only in case.
- Capitalize the first letter of standard acronyms.
- Write only one statement per line
- Use braces around statements that are part of a control structure, even if it is a single statement.

In addition to the above conventions there are certain notations, depending on their respective types and when followed, these notations can enhance readability.

Variables Names

Use Hungarian Notation, which is the most popular notation.

Examples:

sFirstName
iZipCode
lUnitPrice
lDiscountRate
cOrderItems

Alternatively you can use leading or trailing underscores after the name.

Examples:

_firstName
firstName_

Constants

Use uppercase words separated by underscores.

Examples:

MINIMUM_BALANCE
MAX_VALUE
DEFAULT_START_DATE

Collections

Use a name in the plural form representing the type of objects stored by the array.

Examples:

customers
orderItems
aliases

Member Functions
It is a common practice for the first word of a member function name to be a strong, active verb.

Examples:
openAccount()
printMailingLabel()
save()
delete()

Accessor Member Functions (Getters) (Apply to Java only)

Getters are member functions that return the value of a field. You should prefix the word 'get' to the name of the field, unless it is a boolean field and then you prefix 'is' to the name of the field instead of 'get.'
Examples:
getFirstName()
getAccountNumber()
getLostEh()
isPersistent()
isAtEnd()

Mutator Member Functions (Setters) (Apply to Java only)

Setters are member functions that modify the values of a field. You should prefix the word 'set' to the name of the field, regardless of the field type.

Examples:
setFirstName(String aName)
setAccountNumber(int anAccountNumber)
setReasonableGoals(Vector newGoals)
setPersistent(boolean isPersistent)
setAtEnd(boolean isAtEnd)

Constructors

These are member functions that perform any necessary initialization when an object is first created and have the same name as that of the class.

Classes
Should be a noun with the first letter capitalized. Also the first letter of every new word should also be capitalized. Example: HelloWorld.

Interfaces *(Apply to Java only)*

- Should be a noun with the first letter capitalized. Also the first letter of every new word should also be capitalized.
- You can prefix an interface name with '*i*' or postfix it with '*ifc*' to avoid confusion with similarly named classes.

Packages (Apply to Java only)

- Identifiers are separated by periods.
- Local package names begin with an identifier that is not all upper case.
- Global package names begin with the reversed Internet domain name for your organization.
- Package names should be singular.

Components
Use three letter prefixes (Hungarian notation) to make it easier to know what component is being referred.

Examples:

```
btnOK
mnuFile
lstNames
lblPrompt
```

Alternatively, you can use a full English Descriptor postfixed by the widget type.

Examples:

```
okButton
customerList
fileMenu
newFileMenuItem
```

Source Code Style Guidelines
Line Spacing: Line width should not ordinarily exceed 80 characters. Use your best judgment. Tab sizes should be set equal to 2 spaces.

Braces and Indentation: The starting brace can be optionally at the end of the conditional or on the next line aligned with the conditional. The ending brace must be on a separate line and aligned with the conditional. The block of code within braces should be indented.

Examples:

```
while (result.next())
{
        String header = result.getString("SHELTER_POPULATION_CODE");
        String desc = result.getString("SHELTER_POPULATION_DESC");
        String status = result.getString("CODE_ACTIVE_STATUS");
}
```

Documentation
If your program isn't worth documenting, it probably isn't worth running. Write the documentation before you write the code. Avoid decoration, i.e. do not use banner-like comments and always keep your comments simple.

Comments
Comments should add to the clarity of your code. There are three types of Comments.

1. Multi-Line Comments which start with /* and end with */

Examples:

```
/*
    Request and response are the handles from the servlet.
    Use RequestDispatcher to forward request and response to the JSP page.
*/
```

2. Single-line comments start with // and go until the end of the source-code line

Examples:

// obtaining a pooled connection

3. Documentation comments start with /** and end with */ (Apply to Java only)

Examples:

/** This class is used to control the access for the HTS system. This object will *need to be bound to the session object. Depend on the external environment, the *object can be created by using LDAP, databases, or from CRS.
*/

Documenting Fields

To be effective, you need to document:

- Field description
- Document all applicable invariants.
- Concurrency issues.
- Visibility decisions.

Documenting Local Variables

- Document local variables with an single-line comment
- Use local variables for one thing only

Documenting Member Function Headers

Document why something is being done, not just what.

- What and why the member function does what it does.
- What a member function must be passed as parameters.
- What a member function returns.
- Known bugs.
- Any exceptions that a member function throws.
- Visibility decisions.
- How a member function changes the object.
- Include a history of any code changes.
- Examples of how to invoke the member function if appropriate.
- Applicable preconditions and postconditions.
- All concurrency issues.

Documenting Parameters

You should describe:

- What it should be used for
- Any restrictions or preconditions

Documenting Classes

- The purpose of the class
- Known bugs
- The development/maintenance history of the class
- Document applicable invariants
- The concurrency strategy

Documenting Interfaces (Apply to Java only)

- The purpose
- How it should and shouldn't be used

Documenting Packages (Apply to Java only)

- The rationale for the package
- The classes in the package

Documenting Compilation Units

- For files with several classes, list each class
- [OPTIONAL] The file name and/or identifying information
- Copyright information

Internal Documentation

Internally, you should always document:

- Control structures
- Why, as well as what, the code does
- Local variables
- Difficult or complex code
- The processing order
- Document your closing braces

Using These Standards Effectively

- Understand the standards
- Believe in them
- Follow them while you are coding
- Make them part of your quality assurance process
- Adopt the standards that make the most sense for you

Factors That Lead to Successful Code

- Program for people, not the machine
- Design first, then code
- Develop in small steps
- Read, read, read
- Work closely with your users
- Keep your code simple
- Learn common patterns, antipatterns, and idioms